参考資料７

諸外国におけるPIA要否等判断基準

第１　アメリカ

PIA要否基準として、**プライバシーしきい値分析（Privacy Threshold Analysis，以下「PTA」という。）**を採用している。

○　PTAは、システムがPIAやSORN（System of Records Notice）[1]等を必要とするかに係る公的な決定書として必要とされるものである。

○　PTAは3年で失効するため、再認定を受けなければならない。

○　国土安全保障省（DHS）で用いられているPTAの項目は、以下の通り[2]。

①要約情報
- 提出日
- プロジェクト名
- TAFISMA[3]上のシステム名
- コンポーネント名
- プロジェクトマネージャー氏名、メールアドレス、電話番号
- プロジェクトの種類

---

[1] SORNとは、収集される個人情報の種類、個人情報の収集目的、収集元、外部共有の状況、アクセス及び訂正の方法を特定する、連邦官報（Federal Register）において公表される公的な通知のこと。

[2] PTA template（http://www.dhs.gov/xlibrary/assets/privacy/privacy_pta_template.pdf）

[3] 米特有のもの。

□情報技術・情報システム
□法令等　□ひな形その他の情報収集　□その他

②質問事項
・プロジェクトとその目的について記載する
（技術者以外の人が理解できるように記載すること）
・プロジェクトの状況
□新規開発
□既存プロジェクト（当初開発日、最新更新日、更新に関する一般的な説明を記載する）
・誰の情報を収集、処理又は保管するか（該当するものすべてチェックすること）
□DHS 職員□委託先□公衆□該当なし
・SSN（社会保障番号）を利用又は収集するか
□いいえ
□はい（SSN を収集する理由、SSN の機能、SSN を利用又は収集する法的権限）
・個人に関するどのような情報が収集、生成又は保管されるか
・技術/システムの場合は、インフラのみに関連するものか
（例：LAN、WAN）
□いいえ→次の質問に移る
□はい→通信ログを保管しているか
□いいえ→次の質問に移る
□はい→どのような種類のデータがログとして記録されているか（該当するものすべてにチェックすること）
□ヘッダ

□本体→記録されるデータを説明すること

・システムは、個人識別情報について他の DHS システムと接続するか、又は受領若しくは共有するか

□いいえ

□はい→列挙すること

・OCIO[4]による FISMA トラッキングシステム[5]内で認証されているか

□わからない

□いいえ

□はい→

機密性□低□中□高□未定義

完全性□低□中□高□未定義

可用性□低□中□高□未定義

③国土安全保障省プライバシーオフィス記載事項

・国土安全保障省プライバシーオフィスレビュワー氏名

・指定事項

□本システムは、プライバシーセンシティブシステムではない（本システムは個人識別情報を含まない）

□本システムは、プライバシーセンシティブシステムである

システムの分類

□IT システム

□国家的セキュリティシステム

□レガシーシステム

[4] Office of the Chief Information Officer のことと推測される。

[5] 米特有のもの。

□人事システム
□規則
□その他

決定事項
□現時点ではPTAで十分である
□プライバシーコンプライアンス文書決定が進行中である
□現時点ではPIAは要求されない
□PIAが要求される
　□システムは、既存PIAにてカバーされる
　□新しいPIAが要求される
　□PIAの更新が要求される
□現時点ではSORNは要求されない
□SORNが要求される
　□システムは、既存SORNにてカバーされる
　□新しいSORNが要求される
・国土安全保障省プライバシーオフィスのコメント

○　なお、新しいプライバシーリスクを生起するシステム変更もPIAの対象範囲となるが、その具体例として、M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002では以下を挙げている。

①　紙ベースの記録を電子的システムに変換するとき
②　情報収集を匿名化から非匿名化に変更するとき
③　重大なシステム管理の変更（たとえば、複数のデータストアにアクセスできるようなリレーショナルデータベース

技術や Web ベース処理を新たに採用する場合における変更は、データの暴露を起こしやすいオープンな環境や方法を生起する）

④　重大な統合（個人識別情報を保有する政府のデータベースと他のデータベースとの統合、中央化、マッチングその他重大な操作）

⑤　公衆がアクセスするシステムに、ユーザ認証技術（パスワード、電子認証、バイオメトリックなど）を採用するとき

⑥　個人識別情報を含む既存データベースに商業情報源又は公的情報源を体系的に統合するとき（既存の技術を用いてアドホックにかかる情報源に問い合わせを行う場合は、PIA は要求されない）

⑦　省庁間の新たな利用（分野横断的な電子政府行動の場合は、主官庁が PIA を実施すること）

⑧　内部フロー又は収集（情報の新たな、かつ重大な利用や開示をもたらすビジネスプロセスの変更、又は個人識別情報の追加項目のシステムへの統合をもたらすビジネスプロセスの変更）

⑨　データ特徴の変更（個人識別可能な新たな情報が収集に加えられることで、個人のプライバシーに対するリスクがもたらされるとき（健康情報や経済情報の追加など））

第２　オーストラリア

PIA 要否基準として、**しきい値評価（Threshold Assessment）**を採用している。

○　しきい値分析は、PIA が必要かどうか判断するためのものである。どのような場合に PIA を実施しなければならないかに関しての明確なルールはないため、個々のプロジェクトにおいて個別に検討しなければならない。

○　但し、しきい値分析は主に、プロジェクトが個人情報を収集、使用又は開示するか否かを検討するものであり、概して、かかる場合には PIA が必要となる 。なお、個人情報を取り扱わない場合でも、個人情報を使用していないことを示すためやその他の種類のプライバシー（身体的、領域的、通信プライバシーなど）への対応を示すために PIA を実施することは可能 。

○　しきい値評価の項目は以下の通りである[6]。

①組織名
②責任者の連絡先
③プロジェクトの簡単な説明（後記（２）①プロジェクト説明を参照）
④個人情報を収集、使用又は開示するか
　・収集、使用又は開示される個人情報を記載する
　・プライバシーに関する主要な点（例：目的、法的根拠、個人情報の性質・機微性）を記載する
　・プログラム修正の場合は、個人情報の取扱方法に関する変更点を記載する
⑤担当者及び責任者の氏名、署名、日付

[6] Privacy Impact Assessment Guide（http://www.privacy.gov.au/materials/types/download/9509/6590）

第３　イギリス

フルスケールPIAを実施すべきか、スモールスケールPIAを実施すべきかの判断基準として、スクリーニング質問(screening questions) **を設けている。**

	フルスケール PIAの要否基準	スモールスケールPIAの要否基準
Technology 技術	(1) Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?	(1) Does the project involve new or inherently privacy-invasive technologies?
	プライバシーに対し相当適度の侵害をもたらしうる新しい技術を用いるか、又はそのような技術を追加するか	プライバシーに侵害をもたらしうる新しい技術を用いるか、又は本質的にプライバシーに侵害をもたらしうる技術を用いるか
Justification 正当化理由		(2) Is the justification for the new data-handling unclear or unpublished?
		新しくデータを取り扱う理由が不明瞭だったり非公表だったりするか
Identity 識別	(2) Does the project involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?	(3) Does the project involve an additional use of an existing identifier?
	新しい識別子を用いるか、既存識別子の再利用を行うか、侵害的個人識別、個人認証、識別管理プロセスを用いるか ※(2)では、右記(4)と異なり、multiple-purpose identifierは一つの例として挙げられている。	既存識別子を追加的に利用するか
		(4) Does the project involve use of a new identifier for multiple purposes?
		新しい多目的識別子を利用するか

	(3) Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?	(5) Does the project involve new or substantially changed identity authentication requirements that may be intrusive or onerous?
	事業が匿名性を否定する効果をもつか、又は以前は匿名で行えていた取引を本人識別可能な取引に変化させるか	侵害的又は負担になりうる識別認証要件を新しく用いるか、かかる識別認証要件に重大な変更を加えるか
Multiple organisations 複数の組織	(4) Does the project involve multiple organisations, whether they are government agencies (eg in 'joined-up government' initiatives) or private sector organisations (eg as outsourced service providers or as 'business partners')?	
	複数の組織が関わるか。複数の組織が関わる場合、政府機関か民間セクター（外部委託業者など）か	
Data データ	(5) Does the project involve new or significantly changed handling of personal data that is of particular concern to individuals?	
	個人にとって格別の懸念を生じさせるような個人データを新しく取り扱うか、又はかかる点について重大な変更があるか	
	(6) Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database?	(6) Will the project result in the handling of a significant amount of new data about each person, or significant change in existing data-holdings?
	相当量の個人データをデータベースで取り扱うか、又はか	各個人に対し新しいデータを大量に取り扱うこととなるか、又

	かる点について重大な変更があるか	は既存のデータ保持に重大な変更があるか
	(7) Does the project involve new or significantly changed handling of personal data about a large number of individuals?	(7) Will the project result in the handling of new data about a significant number of people, or a significant change in the population coverage?
	多数人の個人データを取り扱うか、又はかかる点について重大な変更があるか	大量の人数の新しいデータを取り扱うか、人口カバレッジに重大な変更があるか
	(8) Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?	(8) Does the project involve new linkage of personal data with data in other collections, or significant change in data linkages? ※linkage には左記行為も含む
	複数の情報源から得た個人データを連結、マッチング、相互参照等行うか、又はかかる点について重大な変更があるか	他に収集されたデータと個人データを新しく結びつけるか、又はデータの結びつけに重大な変更があるか
Exemptions and exceptions 適用除外	(9) Does the project relate to data processing which is in any way exempt from legislative privacy protections?	(15) Will the project give rise to new or changed data-handling that is in any way exempt from legislative privacy protections?
	プライバシー保護法令の適用除外となる事業か	プライバシー保護法令の適用除外となりうるデータ取扱いを新たに行うか、変更するか
	(10) Does the project's justification include significant contributions to public security measures?	
	事業の正当化理由として、国民の安全への多大な寄与を挙げていないか	
	(11) Does the project involve systematic disclosure of personal data to, or access by, third parties that are not	

	subject to comparable privacy regulation? プライバシー規制に服さない第三者へ、個人データをシステマティックに開示したり、かかる第三者が個人データにアクセスできるようにしていないか	
Data handling データ取扱い		(9) Does the project involve new or changed data collection policies or practices that may be unclear or intrusive? 不明瞭もしくは侵害的なデータ収集ポリシーを新しく盛り込むか、不明瞭もしくは侵害的なデータ収集を新しく行うか、またはデータ収集ポリシーもしくはデータ収集を変更して不明瞭もしくは侵害的なものとなるか (10) Does the project involve new or changed data quality assurance processes and standards that may be unclear or unsatisfactory? 不明瞭または不十分なデータ保証プロセス及びデータ保証標準を新たに盛り込むか、またはデータ品質保証プロセス及びデータ保証標準を変更して不明瞭または不十分なものとなるか (11) Does the project involve new or changed data security arrangements that may be unclear or unsatisfactory? 不明瞭または不十分なデータセキュリティを新たに組み込むか、または変更して不明瞭又は不十分なものとなるか (12) Does the project involve new or changed data access or disclosure arrangements that may be unclear or permissive?

		不明瞭または安易になりうるデータアクセスまたは開示を新たに組み込むか、または変更して不明瞭または安易になりうるか
		(13) Does the project involve new or changed data retention arrangements that may be unclear or extensive?
		不明瞭または広汎になりうるデータ保管を新たに組み込むか、または変更して不明瞭または広汎になりうるか
		(14) Does the project involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?
		公開情報の開示方法について、以前よりも容易にデータにアクセスできる方法に変更しているか（？？、但し回答が Yes だとリスクありとされるので、そうすると訳が変？？）

第４　カナダ（連邦）

PIA ガイドラインにて、まず、システムにおいて個人情報の収集、使用または開示が行われるかを確認する。個人情報の収集等が行われる場合は、以下の**チェックリスト**により PIA の実施時期等を検討する。

①以下の行為を行うか
- ・新しいプログラム又はサービスの設計
- ・既存プログラム又はサービスの重大な変更
- ・旧型伝達方法から電子伝達方法へ変更し、顕著なプライバシー問題を有し PIA を実施していない場合

②プログラム上で個人情報の収集、使用又は開示を行うか

③プログラム上で以前よりも機微性の高い個人情報を収集、使用又は開示するか。個人情報の収集方法を、同意に基づく方法から間接的取得方法に変更するか。

④個人のプライバシー権に関する通知又は個人情報の収集、使用及び開示に関する同意取得の機能を設ける必要があるか

⑤プログラム上で、組織内の他のプログラム、他の組織、他の政府又は民間事業者から個人情報を収集するか

⑥プログラムによって生成された個人情報が、当該個人に直接影響を与える決定過程（たとえば、プログラム又はサービスの適格性や執行など）において用いられるか

⑦プログラムによって生成された個人情報が、その他の目的（調査、統計目的なども含む）で用いられるか

⑧当初収集された目的以外のために、個人情報が他の組織との間で共有されるか

⑨新しい共通識別子、又は法令上の根拠なく SIN（社会保障番号）を用いるか

⑩公衆が、プログラム又はサービスに関してプライバシーに対する懸念を有することが予測されるか

⑪個人情報の物理的又は論理的分離に影響を与えたり、個人情報の管理やアクセスコントロールのためのセキュリティ機能に影響を与える変更を、業務システムやインフラに対して行うか